EDUCATIONAL INSTITUTION / NON-PROFIT ORGANIZATION INDIVIDUAL SECURITY PLAN

Subcontractor Name: _____

Subcontract Worker: _____
Worker's Full Name

P.R. / Subcontract #: _____

Type of Clearance Required: ☐ Q ☐ L ☐ No Clearance

Type of Badge Received:
- ☐ LANL Generic Uncleared US Visitor
- ☐ LANL Generic Uncleared US Visitor Escort Required
- ☐ LANL Uncleared Site-specific
- ☐ LANL Uncleared / Cleared Foreign National
- ☐ Uncleared DOE
- ☐ DOE L
- ☐ DOE Q

SECTION I

In the performance of the referenced Subcontract and in order to comply with security requirements for subcontract workers outlined in DOE O 470.4B Chg 1, *Safeguards and Security Program*, LANS, LLC and the Subcontract worker agree to the following Individual Security Plan:

1. Subcontract worker shall comply with all security requirements outlined in this Individual Security Plan as well as any other security requirements discussed and briefed by their LANL host.

2. All non-U.S. citizen foreign national subcontract workers are required to have approval to work on-site from the LANL Foreign Visits and Assignments office PRIOR to their arrival at the Laboratory. They are required to present a valid passport and visa documentation before a badge will be fabricated and issued.

3. All required training shall be completed and documented prior to any work beginning. A record of all required and completed training follows.

Course Required?	Course Title	Date Completed
General Security		
	General Employee Training (GET) - On site 10 or more days	
	LANL Emergency Procedures and Protective Actions - All	
	Annual Security Refresher (ASR) – L & Q-cleared Workers	
	Comprehensive Security Briefing - L & Q-cleared Workers	
	Export Control Fundamentals – Based on SOW	
	Substance Abuse Awareness – All	

Course Required?	Course Title	Date Completed
	Workplace Violence Awareness - All	
Cyber Information Security		
	Initial Information Security Briefing - All Computer Users	
	Annual Information Security Refresher – All Computer users	
Protecting Classified & Sensitive Information		
	Protecting UCNI - Users of Unclassified Controlled Nuclear Information (UCNI) – If access to UCNI will be required	
Physical Security		
	The Outsider – Vault or Vault Type Room User (AIS Escorts)	
	Vault or Vault Type Room User – Vault or Vault Type Room Users	
LANL Site-Specific Training (list as appropriate)		

4. A subcontract worker who will obtain a standard badge (non-Visitor or Generic) such as a DOE Q, DOE L, DOE Uncleared, LANL Uncleared Site-specific, or Cleared/Uncleared Foreign National badge shall successfully pass a drug test no more than 60 days before requesting and obtaining a standard badge.

5. Should the parties to the above referenced change, all applicable Foreign Ownership, Control or Influence (FOCI) security requirements associated with a Q clearance will be immediately applicable as required by DOE/NNSA. [Contact Melissa Abeyta regarding FOCI requirements at 505-665-1624]

6. Any badge provided by LANL under the above subcontract is strictly for use in the performance of the work outlined in this subcontract and the badge shall not be utilized for any other work or activities.

7. Subcontract worker shall notify LANL Personnel Security immediately if access to LANL is no longer required due to termination of subcontract, badge expiration, end of assignment or completion of a visit. Failure to return a badge will result in denial of future badging services to the badge holder.

8. When the subcontract is terminated, any associated security clearance will also be terminated.

By signature below, the responsible LANL line manager (RLM) and Subcontract worker acknowledge that all the security requirements contained herein have been briefed, read and agreed upon. A copy of this ISP shall be provided to the Subcontract worker.

Approved by LANL Manager (RLM)

_____	_____	_____
Printed Name	*Signature*	*Date*

Accepted by Subcontract Worker

_____	_____	_____
Printed Name	*Signature*	*Date*

SECTION II

Additional security requirements that shall be complied with while working for Los Alamos National Laboratory are outlined in the following pages.

Subcontract worker's signature on this Individual Security Plan acknowledges consent to comply with these requirements; in addition to any facility-specific security requirements the LANL host may provide.

General Security

Security Awareness

Laboratory workers should always be vigilant of their surroundings.

Workers should inspect work areas frequently for

- suspicious activities;
- unattended packages; and
- signs of tampering or indications of forced entry into doorways or windows.

In addition to locking parked vehicles, workers should also get in the habit of inspecting their vehicles for suspicious items before entering and driving.

Situations to Report	Whom to Call
Suspicious or unknown persons, particularly those carrying suitcases or other containers or those observing, photographing, or asking questions about site operations or security measures; protesters and unauthorized demonstrations	Protective Force (667-4437) or Security Inquiry Team (665-3505)
Unidentified vehicles parked or operated in a suspicious manner on or near Laboratory facilities	Protective Force (667-4437)
Abandoned packages; low-flying aircraft	Emergency Operations (667-6211) or Protective Force (667-4437)
All other unauthorized activities or anything out of the ordinary	Protective Force (667-4437)

Reporting Security Incidents

All potential and actual incidents of security concern must be reported IMMEDIATELY to the Security Incident Team (SIT) and to your supervisor

Why?

- Timely reporting of incidents is a sign of a healthy security culture at the Laboratory.
- Immediate reporting allows security professionals to help make breaches less severe, address vulnerabilities before they can be exploited, and notify higher authorities at the Laboratory, NNSA, and the Department of Energy (DOE).
- Immediate self-reporting is a means to avoid a security infraction.
- Early reporting allows security professionals to limit the scope of a problem, which then reduces the number of systems that have to be taken down during a breach.
- The SIT has special guidelines to help ease some types of issues related to security incidents that are time sensitive.
- It is better to rely on security professionals who are trained, rather than trying to determine if the incident impacts other systems at the Laboratory. It is not worth accepting that level of responsibility on your own. Just report!

Incidents are bound to occur when humans work with processes. A quick response with appropriate reporting is one way that we as a Laboratory are able to earn the trust of our customers, NNSA and DOE. When incidents occur, pause for a minute and then realize that the best thing to do is report immediately. In this way, you avoid going down a path of "wondering" if it is an incident and end up making a bad decision. Report the incident and immediately transfer the burden of this important and impacting decision to a security professional from the SIT.

Contacts

- Security Incident Team: 665-3505
- After-hours Duty Officer: 949-0156 (pager)

Work Place Violence

Workplace violence consists of hostile or aggressive physical contact with another person, a statement or body gesture that threatens harm to another person, or conduct that would cause a reasonable person to believe that he or she may be harmed.

Preventing Workplace Violence

Know the people with whom you work and notice when their behavior seems out of place or out of character. The following behaviors can be warning signs of potential workplace violence:

- sudden changes in behavior or work pattern such as unwillingness to follow directions;
- yelling, slamming or throwing objects, verbally challenging or intimidating behavior;
- lying or participation in compulsive behaviors like gambling or addictive behaviors involving alcohol or other drugs;
- blaming others and refusing to take personal responsibility for concerning behaviors; and/or
- significant changes in social interactions (i.e., sudden withdrawal or seeming preoccupation with a specific individual or groups).

Reporting Concerning Behavior

Workers should always be alert for worrisome behavior by another employee or others near the workplace. Those with concern should notify the group or higher-level manager about the behavior, particularly if there is a threat of workplace violence.

A supervisor must act when a worker threatens or demonstrates violent behavior by having the worker removed from the workplace and notifying security. The supervisor must also report the incident to Human Resources-Employee Relations.

How to Handle a Violent Situation

If you believe the situation is life threatening or could result in bodily harm, call 911 immediately.

Resources

- Human Resources - Employee Relations, 667-8730
- Security Help Desk, security@lanl.gov, 665-2002

Responding to an Active Shooter

The workplace should never be a dangerous place. Unfortunately, shooting incidents have occurred across the country. In spite of the intense media coverage, such workplace assaults are very rare. Should such an incident occur at the Laboratory, however, employees should know how to respond to protect themselves and their coworkers.

In Case of a Shooting

When you become aware of a workplace shooting occurring or is about to occur:

- Try to stay focused so you can think more clearly and respond more effectively.
- Stay where you are and lock down if possible. Close and lock office doors and hide in your office, perhaps under a desk, to best protect yourself.
- Call 911 if it is safe to reach a phone. Quietly provide any pertinent details that might help responders (such as number of gunmen and number of building occupants). **Do not leave a safe location to look for a phone.**
- **Do not activate fire alarms.** Doing so might create panic and place people in greater danger.
- Emergency situations are unpredictable. There may not be a specific procedure to rely on for guidance. **Use common sense and focus on your safety and the safety of those around you.**

After a Shooting

Do not leave your office or shelter, even if the shooting seems to have stopped. Staying in place will help law enforcement personnel, emergency responders, or hostage negotiators accurately assess the situation and collect evidence more effectively.

Dealing with the Aftermath

The Laboratory will provide grief counselors and other assistance to help survivors should a shooting ever occur on Laboratory property. Workers who experience workplace violence are encouraged to seek help.

Reporting Requirements for Vehicle Accidents

For many years, the Laboratory has conducted substance abuse testing following accidents. Testing protects Los Alamos National Security, LLC, and the employee by, in most cases, ruling out substance abuse as a causal factor. The Laboratory has increasingly focused on vehicle safety following automobile accidents. As part of this effort, the Laboratory is ensuring it obtains timely information to determine if substance abuse testing Is appropriate in any given circumstance.

All workers must notify their managers when involved in a vehicle accident when:

- The worker is driving any government-owned vehicle. including motorized equipment such as a forklift, on or off Laboratory property, or
- The worker is driving any private vehicle (including rental vehicles) within the boundaries of a Laboratory technical area other than TA 00, which comprises downtown Los Alamos and White Rock.

Notification

A worker must notify his or her manager as soon as possible after being involved in a vehicle accident as described above. The manager must coordinate with Personnel Security; In consultation with the manager, Personnel Security wlll determine If testing Is appropriate, based on all circumstances. If the worker's manager is unavailable, the worker must notify the next level manager or Personnel Security.

See *the Substance Abuse Procedure, P732, for details on testing protocols and notification requirements.*

Refusal to be Tested

Consistent with the LANS Procedure on Substance Abuse, P732, a worker who refuses to be tested, will be treated in the same manner as if there is a confirmed positive result.

Resources

- Human Resources-Employee Relations, employee_relations@lanl.gov, 667-8730
- Personnel Security, 667-4264

Training

Course #42095, Substance Abuse Policy and Procedure P732, for all Laboratory workers.

Personnel Security

Substance Abuse Testing & Reporting

Testing Requirements

- In addition to the drug and alcohol testing conducted under our institutional program (see P732 Substance Abuse), drug testing is now being conducted for L- and Q-cleared workers as part of a federally mandated and regulated program (10 CFR 707). **All new L and Q security clearance applicants will be drug tested before a clearance is granted.**
- When work is being performed outside of business hours, drug and/or alcohol testing under reasonable suspicion or post incident/accident can now be performed. Managers are instructed to contact SOC-LA, LANL's Protective Force, for testing procedures.

LANL's Mobile Testing Units

Reporting

In addition to reporting arrests or convictions of any criminal drug statute violations to PS-3, ALL WORKERS are now required to report arrests or convictions of any alcohol-related incidents (e.g., driving under the influence, driving while intoxicated, public intoxication). PS-3 will notify Occupational Medicine (OM-MS). OM-MS may conduct a medical and or psychological evaluation of the worker as part of monitoring for Fitness For Duty or the Human Reliability Program.

Badge Holder Responsibilities

Every Laboratory worker and visitor is badged. Whether cleared or uncleared, badge holders must follow Department of Energy and Laboratory rules regarding protecting their badges. Workers must:

- Remove their badges and protect them from public view off Laboratory-owned, leased, or rented property.
- Not use their badges for identifcation or unofficial purpose (e.g., cashing checks or checking into a hotel when on vacation). Workers must not scan their badges to fax, post on Web sites, or email for any reason. Note: Workers on official Laboratory travel may use their badges to qualify for discounts, provided they do not allow others to make copies of the badges.
- Submit a Notification of Permanent Inactivation of Badge (Form 1672) in person to the Badge Office if their badges are lost or stolen.

The new federal security badge

Q. Can I wear my badge on the Park and Ride bus?
A. Park and Ride is public transportation. Laboratory workers should not wear their badges at bus stops and buses.

Q. Can I wear my badge at the Hot Rocks Cafe?
A. Because Hot Rocks is housed in the Research Park, which is a leased facility adjacent to the Otowi, workers may wear their security badges at the cafe.

Resources
Badge Office, badge@lanl.gov, 667-6901
Security Help Desk, security@lanl.gov, 665-2002

Foreign National Access into LANL Buildings

Foreign national workers and visitors (including those who have US permanent residency status) must be approved by the Office of Counterintelligence/Foreign Visits & Assignments Office (OCI/FVA) prior to their arrival at LANL. A request through the Database for International Visits and Assignments (DIVA) must be approved before foreign nationals access a LANL facility.

If a foreign national needs access to a building not listed on DIVA, his or her host can update the approved DIVA record.

Secure Areas

Access to secure areas by uncleared foreign nationals is generally prohibited. Contact OCI/FVA for guidance with the process as it requires approval of the following: DIVA, Form 1726, Specific Access Agenda, Maps, Escort Forms, and coordination with the Protective Force by OCI/FVA.

Reporting Requirements

Entry into an unauthorized building by a foreign national may be a security event. If a foreign national worker has entered a non-secure or secure LANL building that was not approved in DIVA, it is a potential incident of security concern and must be immediately reported (via secure means) to the Security Inquiry Team (SIT).

Resources

OCI/FVA: 665-1572, foreignvisit@lanl.gov
Security Help Desk: 665-2002, security@lanl.gov
SIT: 665-3505

Unclassified Foreign Visits In Leased Facilities

Laboratory workers must protect government equipment, real property, Controlled Unclassified Information (CUI), and intellectual property by controlling access to leased facilities.

LANL leases privately owned facilities throughout Los Alamos County. Some examples include the Research Park, Pueblo Complex, Central Park Square, and the White Rock Training Center. All leased space are considered Property Protection Area's (PPA), with the exception of the Bradbury Science Museum, which is an Open Area where the general public is allowed.

All non-US visitors and assignees MUST be:

- vetted and approved prior to their arrival and must be processed through the Badge Office for a standard site-specific badge;
- approved and badged prior to their access to ANY Laboratory facilities, whether owned or leased.

DIVA

The Database for International Visits and Assignments (DIVA) is the means by which the Laboratory processes requests to have foreign nationals on Laboratory-owned or -leased property for work or visits. Following DIVA approval, Foreign Visits and Assignments (FV&A) authorizes the Badge Office to issue badges to foreign national visitors.

Non-US visitors are confined to access facilities that are specifically listed on their DIVA records. Hosts may select these areas from the Approved Building List (http://diva.lanl.gov/fva/doc?page=exemption-list-webpage).

Resources

- Foreign Visits and Assigments, 665-1572
- Security Help Desk, security@lanl.gov, 665-2002

Physical Security

Prohibited Articles

Certain articles are prohibited from Laboratory property, including:

- personally owned firearms;
- dangerous weapons; explosives; and pocket, hunting, or other sharp knives with blades longer than 2.5 inches (Note: knives for official Laboratory work or knives used in the preparation of food are not prohibited);
- alcoholic beverages (opened or unopened), including items such as kegs;
- controlled substances (such as illegal drugs and drug paraphernalia, but not prescription medication); and
- items prohibited by local, state or federal laws.

Open vs. Controlled Access Areas

- East Jemez Road (Truck Route) is an open access area during normal security conditions. There are no restrictions on prohibited articles (unless they are illegal under local, state, or federal law) in private vehicles as long as drivers do not drive into Laboratory property.
- Portions of West Jemez Road, Diamond Drive, and Pajarito Road are protected by Vehicle Access Portals (VAPs) but accessible to the public. Workers are allowed to transport prohibited articles (unless they are illegal under local, state, or federal law) on these open roadways. Workers are not allowed to leave these roadways and access Laboratory property while transporting prohibited articles.
- Roads (including the Pajarito Corridor), parking lots, and open space within VAPs that are physically accessible to the public, but posted with "no trespassing" signs, are controlled access areas. Workers are not allowed to introduce prohibited articles in these areas, and vehicles are subject to random inspections by the Protective Force.

Confiscation

Workers found with prohibited articles in their vehicles in controlled access areas (not open access areas) during Protective Force inspections will be immediately escorted off Laboratory property. Prohibited articles may also be confiscated by the Protective Force or Los Alamos Police Department.

Resources

- SAFE-2 Special Projects Team, 665-7467
- Security Help Desk, 665-2002, security@lanl.gov

Random Vehicle Inspections

Inspection Process

- A Protective Force officer will notify a driver to pull over to a search area, which is marked with a sign and set off with traffic control devices.
- An inspection team, which includes a canine team, will inspect the entire vehicle (under the hood and chassis, the inside, and any items that are towed behind or secured to the roof of the vehicle).
- Upon completion of the inspection, the team will either give the driver permission to proceed or secure the vehicle and the surrounding area as necessary.

Important

Workers must cooperate with and follow the instructions of the Protective Force during inspections. Failure to do so may result in a security incident and notification of the Security Inquiry Team and the worker's line management.

Resources

- Security Help Desk, 665-2002, security@lanl.gov
- Security Perimeter Project, spp-questions@lanl.gov

Photography on Laboratory Property

The use of photographic equipment (e.g., video recorders, film and digital cameras, including cell phones with camera) is prohibited on Laboratory property without approval.

Workers who want to take photographs must:

1. Request prior approval by electronically submitting Form 1897PA;
2. Carry a copy of the approved Form 1897PA while taking photographs; and
3. Present the approved Form1897PA to anyone who requests to see it.

Workers who see photography on Laboratory property should:

1. Question anyone taking the photographs;
2. Ask to see the photographer's approved Form 1897PA; and
3. Immediately notify the Protective Force or Security Inquiry Team to report unauthorized photography.

Resources

- For more information, contact the Classified Matter Protection Group at 667-5108.
- To report unauthorized photography, contact the Protective Force at 667-4437 or the Security Inquiry Team at 665-3505.

Information Security

Using Open Source Information

Information that is considered classified by the US Government may appear in the public domain, in print, or in broadcast media. However, such "open source" information does not make classified into unclassified. Workers must ensure that:

- the information is not used or referred to in an unclassified setting without a derivative classifier's review;
- they take care when discussing such information, even among fellow workers (who may not have the required clearance and/or need to know); and
- they take care when combining material from different sources because unclassified information can become classified through compilation or association.

No Comment Policy

If classified information from an open source is found, that fact itself must be protected as classified information. No comment must be made about the accuracy, classification, or technical merit of the information.

Guidance

Mentors and line managers should:

- brief students and other workers about the potential for unauthorized disclosure when using open source information;
- carefully monitor students who are new, uncleared, and only at the Laboratory occasionally and brief them on boundaries about using online information;
- discourage students and workers from using personal email accounts and computers to do their work; and
- if necessary and appropriate, ensure students and workers have the appropriate resources (e.g., access to a classified network) to work securely.

Reporting

Workers must report suspected and actual incidents of potential unauthorized disclosure to the Security Inquiry Team (SIT). Immediate reporting will assist the SIT in mitigating vulnerabilities.

Resources

- Classification Group, 667-5011
- Security Inquiry Team, 665-3505

Official Use Only (OUO) Information

Official Use Only (OUO) is intended to be viewed only by those individuals with a need-to-know.
Ensure OUO is properly marked and protected.

Nonelectronic media
When using OUO, reasonable precautions must be taken to prevent access of OUO information by persons who do not have the need-to-know. When not using it, store OUO matter in a locked receptacle (such as a room, desk, file cabinet, or safe).

Electronic Media
OUO information stored on a computer should have passwords, authentication, and file access control in place for protection.

Email
OUO should be encrypted with NIST-validated encryption software (Entrust). When transmitted within the LANL yellow network, no encryption is required but it is suggested.

Interoffice mail
Use a sealed, opaque envelope with the recipient's address and the words TO BE OPENED BY ADDRESSEE ONLY on the front of the envelope.

Over telecommunications circuits (including fax)
Protect by encryption whenever possible.

Resources
Security Help Desk 665-2002
Entrust webpage http://network.lanl.gov/entrust/index.php

Unclassified Controlled Nuclear Information (UCNI)

Unclassified Controlled Nuclear Information (UCNI) is certain unclassified but sensitive Government information whose unauthorized dissemenation is prohibited under section 148 of the Atomic Energy Act. Such information may concern nuclear material, weapons, components, facilities that have utilized such items, and security relating to such facilities.

Nonelectronic media

When using UCNI, an authorized individual must maintain physical control over the material to prevent unauthorized access. When not using it, store UCNI matter in a locked receptacle (such as a room, desk, file cabinet, or safe) to preclude unauthorized disclosure. The locked receptacle

Electronic media

UCNI stored on a computer should be restricted to only those that have a need to know. Examples of restrictions are passwords, authentication, file access control, encryption, and offline storage.

Over telecommunication circuits (including fax)

Encryption must be used.

Email

When transmitted electronically outside LANL, UCNI must be encrypted with NIST-validated encryption software (Entrust). When transmitted within LANL's yellow network, no encryption is required but it is recommended. It is the sender's responsibility to ensure that the recipient understands the sensitivity of the information and the requirements for protecting that information.

Export Control

Export Control

Export Control is intended to restrict the export of:

- goods and technology that would make a significant contribution to the military potential of another country or combination of countries;
- goods and technology to further the foreign policy of the United States or to fulfill its declared international obligations; and
- goods where necessary to protect the domestic economy from the excessive drain of scarce materials and to reduce the serious inflationary impact of foreign demand.

Deemed Export

One can "export" something to a foreign national without ever leaving the country. Transfer of technology to a foreign national in the US is deemed to be an export to that person's home country.

Violations of Export Control

Export control is regulated by various executive orders and federal statutes and agencies (e.g., the Department of Commerce, Department of State, and Nuclear Regulatory Commission). Both the Laboratory and workers may be liable if export control requirements are violated. Liabilities include (1) criminal sanctions of fines up to $1 million and imprisonment for up to 10 years; (2) civil penalties; or (3) administrative sanctions, such as seizure of the items in question.

Customs Office

The Laboratory's Customs Office is available to help with obtaining licenses, commodity classifications, designating license exceptions, preparing shipping documents, approving all exports of commodities and software from the Laboratory, and maintaining central records of commodity and software exports.

Resources

- Customs Office, 665-2194, customs@lanl.gov
- Classification Office, 665-6413

Cyber Security

Portable Electronic Devices

Portable Electronic Devices (PEDs) can potentially transmit or transport sensitive unclassified and classified information. The Department of Energy identifies two types of PEDs: Portable Electronic Storage Devices (PESDs) and Controlled Articles.

Portable Electronic Storage Devices (PESDs) can store, read, or write nonvolatile information and be plugged into a computer. PESDs, unlike Controlled Articles, are not "stand-alone" devices. PESDs include:

- CD/DVD write drives;
- external hard drives;
- flash memory (i.e., PC cards, SD memory cards); and
- USB memory devices (thumb drives, memory sticks, jump drives).

Controlled Articles are "stand-alone" devices that can record and/or transmit data. Some examples of Controlled Articles are:

- court-ordered devices (e.g., ankle-monitoring device);
- cameras (e.g., cell phones or other multifunction devices, such as a Blackberry, with photographic capability);
- cell phones and personal digital assistants;
- copiers or scanners with hard drives;
- digital audio players (e.g., iPod);
- laptop or palm-top computers;
- some medical devices (e.g., heart monitor); and
- two-way pagers and radios.

IMPORTANT

Approval to use PEDs on Laboratory property depends on their ownership (personal vs. government-owned), the security requirements of an area, and the risks associated with them.

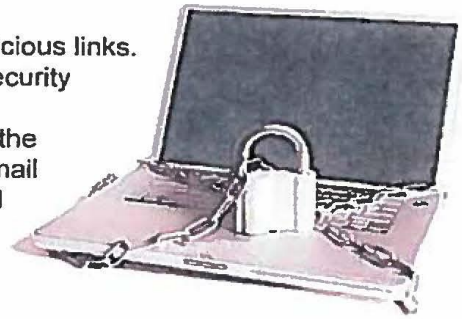
Resources

Information (Cyber) Security Help Desk, 665-1795, cybersecurity@lanl.gov
Security Help Desk, 665-2002, security@lanl.gov

Protecting Your Computer

The Laboratory's Yellow network prevents most cyber attacks. Computer users are an integral part of Yellow network defenses and must ensure their own systems are protected.

Steps to Take



- Do not open unknown email attachments or click on suspicious links.
- Download and install the most recent operating system security patches.
- Ensure an anti-virus application is installed, updated with the latest definitions, and functioning to frequently scan (1) email for viruses, (2) all files being accessed by the system, and (3) all files on the system.

Passwords

Wherever possible, a token card (CRYPTOCard) that generates a one-time passcode should be used for authentication. When a token card cannot be used, creating strong passwords is important in preventing unauthorized access to your computer. Reusable passwords:

- must be a minimum of 8 characters and be changed at least every 180 days;
- must contain a variety of characters (upper-case letters, lower-case letters, numbers, and symbols);
- cannot be names or common words (those found in a dictionary); and
- must never be shared.

Reporting an Information Security Incident

Report all potential information security incidents to the Security Inquiry Team (SIT) at 505-665-3505. After hours or on weekends, page the On-call Duty Officer at 505-949-0156.

Send questions regarding network security to csirt@lanl.gov

Computer User Responsibilities

Computer users are the most important component of the Laboratory's information security program. Heeding the following guidelines will help protect the Laboratory's information assets.

- Get to know your Organizational Computer Security Representative (OCSR) and Systems Security Officer (SSO).
  Visit http://int.lanl.gov/security/cyber/docs/ocsr_isso_list.xls
- Complete required initial and annual information security training:
  http://int.lanl.gov/security/cyber/training/training.shtml
- Know the sensitivity level of the data you process and how to protect that data.
- Understand the "need-to-know" concept before you share information with others.
- Recognize when a computer security incident has occurred and promptly report it to the Security Inquiry Team (SIT) at 665-3505 and your responsible line manager.

- Enable screensaver protections whenever you're away from your computer. Configure your system to automatically engage the screensaver after 15 minutes of inactivity.
- Ensure virus protection software is installed on your system(s) and update definition files at least weekly.
- Follow the established guidelines for destroying data and salvaging computer equipment. Coordinate these activities with your OCSR and property administrator.

Resources
Information Security Website: http://int.lanl.gov/security/cyber/
Contact: cybersecurity@lanl.gov, 665-1795

Protecting Emails and Attachments

Workers must ensure that email containing classified information is not transmitted over unclassified email channels.

Review Before Sending

Review the entire content (text in email and attachments) to verify that it does not contain classified information. If the email could potentially contain classified information, have a derivative classifier (DC) review it.

Emails without Classified Information

If the email does not contain classified information, it can be sent over unclassified email channels. However, keep in mind that emails with controlled unclassified information (CUI), such as Official Use Only (OUO), Unclassified Controlled Nuclear Information (UCNI), and Personally Identifiable Information (PII), have additional requirements:

- **OUO: Indicate OUO on the first line before the body of the text.**
- **UCNI: When transmitted electronically outside LANL, UCNI must be encrypted with NIST-validated encryption software (Entrust). When transmitted within LANL's yellow network, no encryption is required but it is recommended.**
- **PII: Emails containing PII must be encrypted before sending outside the Laboratory.**

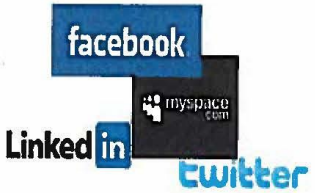
Remember: **Compilation of one or more unclassified attachments and a string of unclassified emails may make the entirety of an email classified.**

Resources

- **Classification Group, 7-5011**
- **Security Help Desk, 5-2002 or security@lanl.gov**
- **Security Inquiry Team, 5-3505**

Social Networking, Privacy and Computer Security

Laboratory workers should be especially careful of what they post in social networking sites. Those who put identifying information online, for example, risk potential unauthorized disclosure and opening themselves up to elicitation by hostile interests.



Some Tips for Privacy

You have little control over your personal information once you post it online. Keep the following in mind:

- Consider your "friends." Before allowing a friend request, think about how information you post will be used, viewed, and shared with others, even those that are not on your list.
- Review the networking sites' privacy policy.
- Make sure you understand how to use the sites' privacy settings — and use them.
- Safeguard your personal information, such as date of birth, personal or work email addresses, and location.
- Do not share details about your Laboratory work.

Some Tips for Computer Security

Spam and malware on social networking sites are on the rise, which can put your computer, network infrastructures, and sensitive data at risk. Remember:

- Run updated virus protection software regularly.
- Delete cookies every time you leave a social networking site.
- Be careful of pop-up windows and links. Verify their legitimacy before clicking on them.
- Avoid accessing social networking sites from your work computer for non-business-related reasons.

Resources

- Cyber Security Help Desk, cybersecurity@lanl.gov
- Organizational Computer Security Representatives, http://int.lanl.gov/security/cyber/docs/ocsr_isso_list.xls
- Security Help Desk, 665-2002, security@lanl.gov

Wireless Networking

Restrictions on wireless networking (802.11) vary by area:

- **Public Access Areas**
  The use of wireless networking, Bluetooth, and cell phones is allowed in areas accessible by the public (within the identified publicly accessible portions of buildings and in public access areas outside buildings, such as roadways, sidewalks, and parking lots).
- **Property Protection Areas (PPAs)**
  The use of cell phones is typically allowed in PPAs (always check local restrictions). However, the use of wireless networking and Bluetooth is prohibited unless approved by the National Nuclear Security Administration (NNSA).
- **Limited Areas**
  The use of wireless networking, Bluetooth, and cell phones is prohibited in Limited Areas unless approved by the NNSA.

Other Wireless Protocols

Radio frequency (RF) and infrared (IR) data communications are allowed in **SOME** instances:

- IR data communications and wireless keyboards are allowed in PPAs on unclassified systems that do not process sensitive information. They are prohibited in Limited Areas.
- RF keyboards are prohibited in all LANL areas.
- IR and RF wireless mice that do NOT use Bluetooth are allowed on unclassified systems where there is no classified processing (unclassified computing environment).
- RF and IR remote controls are allowed on unclassified presentation equipment in unclassified workspaces without restrictions; they are prohibited on classified computers (IR and RF controls are permitted to control classified projectors).

Obtaining Approval for Wireless Devices

Contact the Wireless Team by e-mailing wireless@lanl.gov.

Resource

Information Security (Cyber) Help Desk, cybersecurity@lanl.gov